Exhibit to Data Center Services Service Component Provider Master Services Agreement

DIR Contract No. DIR-DCS-SCP-MSA-002

Between

The State of Texas, acting by and through the Texas Department of Information Resources

and

Atos IT Governmental Outsourcing Services, LLC (formerly called XBS Disposition Subsidiary Two, LLC)

Appendix 7 to Eleventh Amendment
of

Exhibit 2.3.1
Server Services – Semi-Managed
Statement of Work

May 31, 2016

TABLE OF CONTENTS

A.0 SERVICE REQUIREMENTS 6
A.1 Operations 6
A.1.1 DCS Customer Physical Security Administration 7
A.2 Technical Support 7
A.2.1 General Technical Support 7
A.2.2 System Management 7
A.3 Online Storage and Backup Management 8
A.3.1 Storage and Backup Architecture 8
A.3.2 Engineering 8
A.3.3 Operations and Processing 9
A.3.4 Backup and Recovery Services 10
A.3.5 Administration 10
A.6 External Storage Media Management – (Consolidated) 11
A.6.1 Operations and Processing 11
A.6.2 Administration 11
A.6.3 Off-Site Media Storage Management 12
A.7 External Storage Media Management – (Non-Consolidated) 12
A.7.1 Operations and Processing 12
A.7.2 Administration 13
A.7.3 Off-Site Media Storage Management 13
A.8 Intrusion Prevention 15

EXHIBIT 2.3.1
SERVER SERVICES SEMI-MANAGED STATEMENT OF WORK

Update Methodology to Exhibit 2.3.1

The following update methodology is incorporated as part of **Exhibit 2.3.1**:

Title	Methodology for Updating Exhibit
Exhibit 2.3.1 Server Services Semi-Managed SOW	**Exhibit 2.3.1** may only be modified by formal amendment, in accordance with **Section 21.7** of the MSA.

Introduction

This Statement of Work describes the solution for Semi-Managed Server Services that are provided in Consolidated, Non-Consolidated, and Cloud Service Provider Locations. Semi-Managed services consist of the following:

1. Hardware and virtual container management
2. OS license management if purchased by Service Provider
3. OS patching per the default schedule for the OS type
4. Security Services which include anti-virus, vulnerability testing, logging and security event management

The following services are provided if the DCS Customer purchases the optional Resource Unit:

1. SAN storage and management and replication
2. Backup and backup management
3. VPN
4. Network WAN acceleration (Non-Consolidated only)

The following services are not offered for Semi-Managed Services:

1. OS monitoring
2. OS management if the OS license is purchased by the DCS Customer
3. OS management, including work orders, incidents and agency requested CRQs
4. OS clustering support
5. Optional security services which include HIDS/HIPS
6. Database management services
7. Middleware services
8. Disaster Recovery

9. Load balancing

Service Provider will provide a solution that supports all of the business processes described in this Statement of Work and its Attachments, and that all Services, unless otherwise specifically stated, are included in the Charges.

This Exhibit sets forth the Services that the Service Provider will provide, as of Year 5 unless otherwise specified, for all Services that affect Application and Utility Servers described this Exhibit.

Service Provider will be responsive to the current and future requirements of DIR and DCS Customers, by proactively anticipating needs, and adjusting Services accordingly within the Charges. Requirements for New Services will be handled in accordance with **Section 11.5** of the Agreement and Service Provider will work with DIR to assess the impact of these requirements on DIR's and DCS Customers' operating environment and supported Applications in accordance with the terms of the Agreement.

The Service Provider is also required to provide the Services in **Exhibit 2.1.2** in conjunction with the Services described in this Exhibit.

Service Management

DIR bases its Service Management practices on the Information Technology Infrastructure Library (ITIL), a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. Accordingly, DIR requires that Service Provider Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 foundation with ITIL v3 guidance in select functional areas (e.g. Request Management and Fulfillment) with the expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual.

Service Provider responsibilities include:

1. Intentionally deploy and actively manage a set of Service support processes and Service delivery processes that are based on ITIL guidance to enable consistent management of process-driven IT services seamlessly across a variable number of environments and among DCS Service Providers.
2. Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR and DCS Customers and other DCS Service Providers.
3. Execute detailed activities and tasks that are common to IT service operation and maintenance according to the guidance set out in the policies and procedures described in **Exhibit 2.1.2**, including the broader guidance provided regarding the ITIL-based Service Management processes.
4. Design processes to enable the effective monitoring and reporting of the IT services in a Multi-Supplier Environment.
5. Ensure that enterprise processes (e.g. Change Management, Configuration Management, Problem Management) are followed across the DCS Service Provider and Third Party Vendor(s) processes.
6. Coordinate the execution of all the processes across the Service Provider, DIR, DCS Customers, and all Service Component Providers in order that all the individual components that make up the IT Services are managed in an end-to-end manner.

A.0 SERVICE REQUIREMENTS

All activities required to provide the Services set forth in this SOW, including project-related support activities, are included in the Charges.

A.1 Operations

Service Provider responsibilities include:

1. Assume responsibility for the following requirements associated with Application, Utility and Infrastructure Servers, regardless of the physical location of the Equipment, whether located in a Consolidated Data Center, Non-Consolidated Location or Cloud Service Provider Location.
2. Assume responsibility for all master and subordinate console functions.
3. Issue operator commands to control all In-Scope computer platforms throughout the organization.
4. Assume the responsibility for and perform all monitoring activities associated with anti-virus software. operations:
5. Where practicable, provide for automated scheduling of backups.
6. Restore archived or deleted files upon Authorized User’s request.
7. Maintain, administer, and provide necessary automated tools and processes for systems management to the extent available in the DIR-approved tool suite or as required to be delivered by the Service Provider elsewhere in the Agreement.
8. Maintain and update the operational documentation for all semi-managed services.
9. Coordinate with DCS Customer LAN support groups as required for LAN services in Remote locations.
10. Provide, update and maintain a DSL (Definitive Software Library) including references to physical media, license key information, etc. for all server software required to recover or rebuild a server.
11. Install and support sufficient server resources (e.g. data storage, processing capacity, and memory), as directed by DCS Customers.
12. Utilize timing sources as directed by DIR, and as required.
13. Provide Network Time Protocol (NTP) services to DIR and DCS Customers.
14. Assist DCS Customers with data file recovery associated with optional backup services.
15. Provide assistance in analyzing and correcting all CDC network LAN problems that may be associated with Server processing.
16. Maintain and update the documentation for all Server operations procedures and services, including SMMs and excluding runbooks.
17. Provide node/host information, and check and reset ports.
18. Provide remote Software distribution required for semi-managed services.

A.1.1 DCS Customer Physical Security Administration

In addition to the requirements as identified in **Exhibit 17**, Service Provider responsibilities:

1. For Legacy Data Centers for which the Service Provider has operational responsibilities the Service Provider will:
    - 1.1. Recommend supplemental physical security standards and procedures to increase the overall level of security as necessary in the locations and facilities operated by Service Provider.
    - 1.2. Implement such supplemental standards and procedures to be consistent with similar security provisions maintained by first tier providers of services that are the same as or similar to the Services.
    - 1.3. Obtain DCS Customer's approval prior to implementing any supplemental physical security provisions at DCS Customer facilities.
    - 1.4. Comply with DCS Customer's physical security requirements at Legacy Data Centers and Business Offices.

A.2 Technical Support

Service Provider responsibilities include:

1. Provide all technical system support and reporting for storage management for all media.
2. Install and maintain Operating System, as per Optional Services selected.
3. Install and maintain applicable tools, as per Optional Services selected.

A.2.1 General Technical Support

Service Provider responsibilities include the following:

1. Provide appropriate response to incidents and problems and continued support through resolution as required in order to meet scheduled availability.
2. Monitor data storage media.
3. Enforce documentation standards in compliance with Service Management Manual directives.
4. Develop and maintain technical and functional specifications and requirements for all environments and related interfaces.
5. Install, tailor, maintain, and provide ongoing support for Operating System products.
6. Manage, prioritize, and coordinate all preventive and remedial maintenance and updates for System Software.

A.2.2 System Management

Service Provider responsibilities include:

1. Provide, install and utilize tools and processes to allow automated and remote systems management of the Server environment based on optional services selected.
2. Such tools and processes will include:
    - 2.1. Network and system monitoring and control protocols

2.2. Configuration Discovery

2.3. Patch Management

3. Provide the functionality and necessary Software to allow detection, monitoring, and removal of malicious code and/or unauthorized code from all Servers at a level addressing all common platforms (e.g. file systems, email, instant messaging) generally susceptible to malicious code.

A.3 Online Storage and Backup Management

A.3.1 Storage and Backup Architecture

If the DCS Customer selects the optional SAN and Backup services, Service Provider responsibilities consist of:

1. Provide the architecture, design, and planning processes for the development and installation of a Storage and Backup infrastructure that satisfies the needs of all aspects of the business.

1. Remain current in the knowledge and use of data storage technology and management products.

2. Develop and maintain strategies for the deployment and implementation of Storage and Backup solutions in both Consolidated Data Center and Non-Consolidated Service Locations.

3. Coordinate all aspects of Storage and Backup based architecture, design, and planning throughout DIR.

4. Provide and coordinate a Storage and Backup planning interface to all business units and project managers.

A.3.2 Engineering

Service Provider responsibilities consist of:

1. Provide a robust and highly available Storage and Backup infrastructure. Update the Storage and Backup infrastructure as new tools and technology are available that would improve DIR’s or DCS Customers’ business processes and performance

2. Investigate incidents and problems that require an in-depth technical understanding per Incident Management and Problem Management process guidelines.

3. Provide in-depth analysis of operations data environment on behalf of availability management, for example, to assist in service outage investigations.

4. Identify opportunities for continual improvement, through knowledge management and constant skill review.

5. Monitor availability and capacity for backup infrastructure, storage and storage media.

6. Educate and train the operational staff in the use of analysis tools and processes, where appropriate.

7. Plan and prepare for changes in capacity requirements.

8. Participate in scheduled disaster recovery tests.

9. Manage Service Provider relationships and provide a technical interface to other project managers and vendors.

10. Provide evaluations and recommendations for new tools and technologies.

11. Establish and maintain the alerting mechanisms and monitoring systems.

12. Perform testing and benchmarking of new infrastructure or tools prior to deployment into production.
13. Create handover documentation, training, diagnostic scripts, and operational procedures for the operations group.
14. Implement performance and configuration tuning of the Storage and Backup infrastructure in conjunction with Capacity Management and Change Management.
15. Establish system tuning and performance processes.
16. Provide appropriate security measures for the Storage and Backup infrastructure.
17. Document the backup, recovery, retention, and archival requirements of DIR and DCS Customers, as specified in the Service Management Manual.

A.3.3 Operations and Processing

Service Provider responsibilities consist of:

1. Perform successful backups of DIR and DCS Customers systems, in compliance with Service Management Manual.
    - 1.1. Coordinate backup processing with DCS Customers in any situation with the potential to negatively impact operational performance.
2. Remain current in the knowledge and use of data storage technology and management products.
3. Perform online storage tuning.
4. Provide event, warning, alert, and alarm processing and management.
5. Provide resolution of all event, warning, alert, and alarm messages.
    - 5.1. Notify DCS Customers as appropriate on alert notifications.
    - 5.2. Proactively create Incident Records and resolve backup Problems.
6. Interface with the Incident Management and Problem Management processes and liaise will all parties supporting incident and problem resolution.
7. Provide Storage and Backup infrastructure configuration maintenance.
8. Instigate improvement or remedial activities in operational processes under the control of Change Management.
9. Assign and initialize storage as required for performance of the Services.
10. Determine file, data set, and volume placement.
11. Conduct routine monitoring using Software tools to measure the efficiency of online storage access, and take corrective action as needed (including performance adjustments to Equipment and Software, or file placement as required to maximize service).
12. Periodically (but not less than quarterly) retrieve and test all backup media types and verify that the data can be restored in a usable fashion.
13. Coordinate with DCS Customers to periodically (but not less than quarterly) perform production recovery testing of DCS Customers data.
14. Provide compression options for disk
15. Support and manage encryption as required by DCS Customer.

A.3.4 Backup and Recovery Services

Service Provider responsibilities consist of:

1. Assume responsibility for DIR's and DCS Customers' system data backup and recovery requirements for Non-Consolidated Service Locations and Consolidated Data Centers.
2. Provide database backup options (e.g. online, offline, compressed) as required by DIR and DCS Customers.
3. Perform backup and recovery functions utilizing available techniques whether standard tool sets or legacy environment tools (e.g. system state backup, fast recovery) options.
4. Provide Backup of Catalogs/Indexes/log files of data backup.
5. Perform systems data backup and recovery of all Service Provider tools and infrastructure components to ensure the integrity and availability of the operational environments which support DCS Customer Applications to meet daily service and DR commitments.
6. Provide reporting on backups and backup infrastructure (e.g. success/failure, schedules, retention, targets, offsite, archive, tape media).
   - 6.1. Ensure backup schedules correctly reflect the Application schedule requirements, retention requirements, and target directory requirements.
   - 6.2. Regularly validate the Application schedule, retention, and target directory requirements.
   - 6.3. Provide the schedule, retention, and target information as implemented in the CMDB and backup systems to the DCS Customer, as requested.
   - 6.4. Review backup schedule and Application schedule with DCS Customer annually.
7. Establish a process by which Authorized Users can request recovery of data or files, and document the process in **Attachment 6-B**.

A.3.5 Administration

Service Provider responsibilities consist of:

1. Manage online storage thresholds and data archives.
2. Monitor user directories for file inactivity and report monthly.
3. Monitor and maintain file directories and catalogs and report monthly.
4. Provide online storage compaction as needed and as possible within production processing schedules.
5. Provide data migration/archive management, including the migration of media to more current technology to maintain technology currency.
   - 5.1. Coordinate with DCS Customer, as requested, to define and implement disk to tape data archival policies for Application Servers.
   - 5.2. Coordinate with DCS Customer, as requested, and in compliance with the Service Management Manual the creation and handling of tapes identified as Do Not Destroy (DND).
6. Provide documentation support and maintenance.
7. Provide and support file system quota management on file servers as required by DCS Customer.

A.6 External Storage Media Management – (Consolidated)

A.6.1 Operations and Processing

Service Provider responsibilities are for the Consolidated Data Centers and consist of:

1. Coordinate with Data Center Component Provider for operational responsibilities for all External Storage Media management functions, both on-site and off-site, for External Storage Media library operations and administration.
2. Utilize efficient and effective storage media, tools, and processes for DCS Customers' data and programs.
3. Coordinate with DCS Service Providers and other Third Party Vendors to recycle media regularly, manage media replacement, and recopy media to provide data integrity and quality.
4. Periodically (but not less than quarterly) coordinate the retrieval and test of all backup media types and verify data can be restored in a usable fashion and report results.
5. Coordinate with the Data Center Component Provider to wipe/erase the data and configuration information resident on media, prior to disposal or re-use, and in accordance with TAC 202.
6. Provide systems administration and support for media libraries and library management systems.
7. Coordinate with the Data Center Component Provider for the provision of all External Media Storage handling (e.g. tape mounts, physical tape library, tape retrieval) functions required in the Consolidated Data Centers.
8. Coordinate the creation and handling of tapes identified as Do Not Destroy (DND) with DCS Customers and the Data Center Component Provider, as requested, and in compliance with the Service Management Manual.

A.6.2 Administration

Service Provider responsibilities are for the Consolidated Data Centers and consist of:

1. Maintain a database cataloging the archival system for the media libraries.
2. Monitor External Storage Media Equipment in case of malfunction, and initiate corrective action with other DCS Service Providers in accordance with established procedures.
3. Maintain the integrity of External Storage Media libraries system.
4. Monitor External Storage Media for reliability and minimization of read/write errors during the entire period of retention.
5. Monitor and report on External Storage Media usage.
6. Monitor External Storage Media in coordination with the Data Center Component Provider to comply with DIR, DCS Customers and applicable government requirements and reporting.
7. Provide External Storage Media (e.g. cartridges or reel tapes) as required for the Services.
8. Follow, maintain, and update procedures in the Service Management Manual, described in **Attachment 6-B**, which governs cycling/rotation of External Storage Media, External Storage Media management, and External Storage Media retention periods, in accordance with DIR's and DCS Customers' Security Policies, MSI guidelines and with attention to auditing purposes.
9. Manage designated encryption keys for the environment.

A.6.3 Off-Site Media Storage Management

Service Provider responsibilities are for the Consolidated Data Centers and consist of:

1. Document operational process and procedures for off-site rotation in the Service Management Manual, including coordination with the DCS Customer and Data Center Component Provider as required.
2. Work with DCS Customers and Data Center Component Provider to ensure that off-site rotation is provided for all Service media.

A.7 External Storage Media Management – (Non-Consolidated)

A.7.1 Operations and Processing

Service Provider responsibilities are for the Non-Consolidated Service Locations unless otherwise stated and consist of:

1. Assume operational responsibilities for all External Storage Media management functions, both on-site and off-site, for External Storage Media library operations and administration in Non-Consolidated Service Locations.
2. Utilize efficient and effective storage media, tools, and processes for DCS Customers' data and programs.
3. Recycle media regularly, manage media replacement, and recopy media to provide data integrity and quality.
4. Retrieve External Storage Media from on-site and off-site storage as requested by DIR and DCS Customers or as required in an emergency.
5. Wipe and erase the data and configuration information resident on media, prior to disposal or re-use, and in accordance with TAC 202.
6. Dispose of retired media in an environmentally sound manner after purging any DIR or DCS Customer data using State and/or Federal guidelines/policies prior to disposing of media in accordance with TAC 202.
7. Operate and support media libraries and library management systems as required to provide the Services.
8. Perform External Storage Media handling (e.g. tape mounts, physical tape library, tape retrieval) to support operational activities at sites staffed by Service Provider personnel.
9. Properly clean and maintain Equipment to minimize problems and outages, at intervals established with DIR or in compliance with stated and written specifications.
10. At Business Offices, coordinate with other parties (e.g. Third Party Vendor or DCS Customer) to:
    - 10.1. Establish processes and procedures for proper handling of External Storage Media with the other parties; and
    - 10.2. Direct the other parties' personnel to perform External Storage Media mounts.
11. Coordinate the creation and handling of tapes identified as Do Not Destroy (DND) with DCS Customers and the Data Center Component Provider, as requested, and in compliance with the Service Management Manual.

12. Recopy External Storage Media to support minimization of read/write errors, including Refresh to new media per scheduled retirement guidelines, and/or to recover corrupted data.
13. Initialize new External Storage Media.
14. Periodically (but not less than quarterly) retrieve and test all backup media types and verify data can be restored in a usable fashion and report results.

A.7.2 Administration

Service Provider responsibilities are for the Non-Consolidated Service Locations unless otherwise stated and consist of:

1. Maintain a database cataloging the archival system for the media libraries.
2. Monitor External Storage Media Equipment in case of malfunction, and initiate corrective action in accordance with established procedures.
3. Maintain the integrity of External Storage Media libraries system.
4. Monitor External Storage Media for reliability and minimization of read/write errors during the entire period of retention.
5. Monitor and report on External Storage Media usage and provide usage information to DIR and DCS Customers as set forth in the Service Management Manual.
6. Monitor External Storage Media to comply with DIR, DCS Customers and applicable government requirements and reporting.
7. Provide External Storage Media (e.g. cartridges or reel tapes) as required for the Services.
8. Provide and maintain adequate supplies for the External Storage Media.
9. Follow, maintain, and update procedures in the Service Management Manual, described in **Attachment 6-B**, which governs cycling/rotation of External Storage Media, External Storage Media management, and External Storage Media retention periods, in accordance with DIR's and DCS Customers' Security Policies, MSI guidelines and with attention to auditing purposes.
10. Maintain an existing inventory control system to properly manage External Storage Media in storage and prepare them for shipment to the contingency site.
11. Provide media racks and space for media supporting In-Scope IT environments.
12. Perform Audits of media locations as required per DCS Customer and Service Management Manual Guidelines.
13. Manage designated encryption keys for the environment.

A.7.3 Off-Site Media Storage Management

Service Provider responsibilities are for the Non-Consolidated Service Locations and consist of:

1. Assume operational responsibility for off-site media storage, for all Non-Consolidated Service Locations as designated by DIR and DCS Customers, including:
   - 1.1. Integrity checking.
   - 1.2. Definition of storage requirements.
   - 1.3. Manage off-site vaulting of data on media as scheduled.
   - 1.4. Cataloging off-site content.

1.5. Retrieving backup tapes.

2. Compliance with DIR's, DCS Customers' and/or applicable government requirements.

3. Develop requirements, procedures, and standards for off-site storage, in consultation with DIR and DCS Customers, and obtain approval from DIR. DIR will have the right to request modifications to such procedures as required.

4. Store External Storage Media and business-recovery-related paper documentation at secure off-site vault storage. Off-site vault storage also includes External Storage Media business recovery functions, such as packaging and transportation to and from storage and contingency sites as defined in **Exhibit 15**.

5. Provide off-site vault storage in a physically and environmentally controlled and protected area with appropriate fire protection and with multiple layers of physical security designed to prevent unauthorized access as defined in **Exhibit 17**.

6. Follow off-site External Storage Media storage procedures, including:

6.1. Provide secure off-site transport containers.

6.2. Prepare media for off-site storage or to go to other Third Parties as requested by DIR or DCS Customers, or as otherwise required.

6.3. Log and track all physical External Storage Media in and out of the Non-Consolidated Service Locations.

6.4. Ship and receive media to and from the off-site storage location(s) on a daily basis, or as required.

6.5. Support ad hoc requests for tape retrieval from off-site locations in a timely manner.

6.6. Maintain the rotation of the External Storage Media that is required for off-site storage.

6.7. Return media as required to the originating DIR or DCS Customer Location.

6.8. Transport materials to and from off-site storage in secured environmentally controlled vehicles operated by bonded personnel, or as agreed to by DIR.

6.9. Audit the off-site vendor for compliance and control procedures, and provide an audit report to DIR.

6.10. Maintain the integrity of data shipped to off-site storage.

6.11. Manage Third Party Vendors that provide off-site storage services, and notify DIR and affected DCS Customers of any problems.

6.12. Advise DIR of any modifications to agreements with Third Party Vendors that would improve the efficiency of the Services or otherwise benefit DIR or DCS Customers.

6.13. Manage and provide a daily reconciliation of media that is moved to and from offsite storage to ensure that media flagged for movement is properly moved and logged in the appropriate media tracking and inventory systems.

6.14. Manage and provide a reconciliation of all media that is removed from off-site storage following scheduled DR tests and return of media to either off-site storage or the on-site media library.

6.15. Provide an emergency media return process.

6.16. Comply with, and review compliance with, physical specifications, retention periods, and security.

A.8 Intrusion Prevention

Service Provider's responsibilities consist of the following for host-based firewall Intrusion Prevention systems:

1. Install, update, and configure Intrusion Systems as requested by DIR or DCS Customers.
2. Monitor all Intrusion Systems from central logging system, and provide appropriate response to alerts from Systems based upon mutually agreed procedures as defined in the Service Management Manual.
   - 2.1. Provide immediate notification and historical reporting to DIR and DCS Customers per guidelines in the Service Management Manual.
3. Install as needed or as directed by DIR or DCS Customers, known high-risk updates as defined by intrusion systems manufacturer to intrusion system Software within 4 hours or less after such updates are made available to Service Provider (or qualified Third-Party Vendors selected by Service Provider) and approved by DIR or DCS Customers.